CREATE-IoT

European Large-Scale Pilots Programme

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IOT4SCC: Joint Workshop on IoT for Smart Cities & Communities Platform Convergence: Breakout C, 7 June 2018

Outline on Session on Personal Data Protection Strategies and Guidelines

European Large-Scale Pilots Programme

Session 1 (12.30 - 13.30)

- Citizen viewpoint for smart cities
  - Mara Balestrami, Ideas for change
- Privacy-by-design viewpoint for smart cities
  - Antonio Kung, Trialog
- Introduction to smart city use case session
- Selection of smart city use case

Session 2 (14.30-15.30)

- Legal and ethical compliance viewpoint for smart cities
  - Pasquale Annicchino, Archimede Solutions
- Smart city use case session
  - Breaches
  - Threats and consequences
  - Measures
- Conclusion

Citizen viewpoint for smart cities

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Mara Balestrami, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Privacy-by-design Viewpoint for Smart Cities

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Antonio Kung

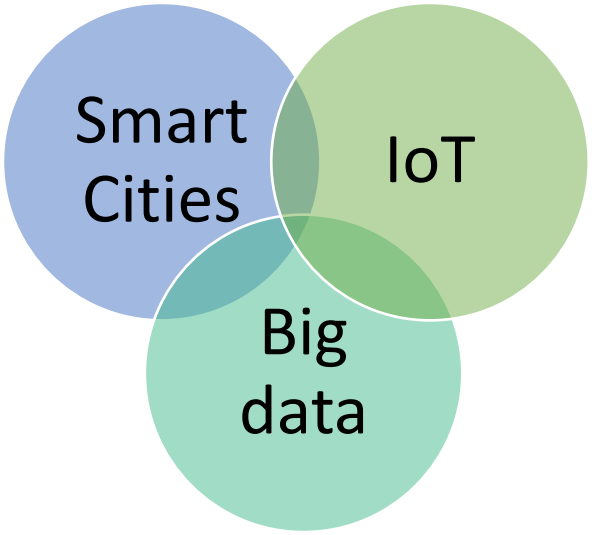
European Large-Scale Pilots Programme

- European projects: PRIPARE, Create-IoT…
- IPEN wiki (ipen.trialog.com)
- EIP-SCC Citizen approach to data: privacy-by-design
  - Workshop London (March 2017)
  - Workshop Milan (July 2017)
  - Workshop Brussels – Eurocities (January 2018)
- Involved in standardisation
  - ISO/IEC 27570 - Privacy guidelines for smart cities
  - ISO/IEC 27030 - Security and privacy guidelines for IoT
  - ISO/IEC 27550 - Privacy engineering for system life cycle processes
  - ISO/IEC 30147 - Methodology for implementing and maintaining trustworthiness of IoT systems and services
  - ISO/IEC 20547-4 – Big data reference architecture – Security and privacy

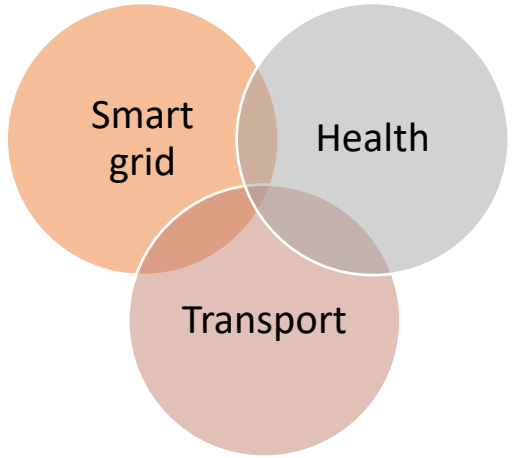
Co-funded by the European Commission

ICT Trend towards Complex Ecosystems

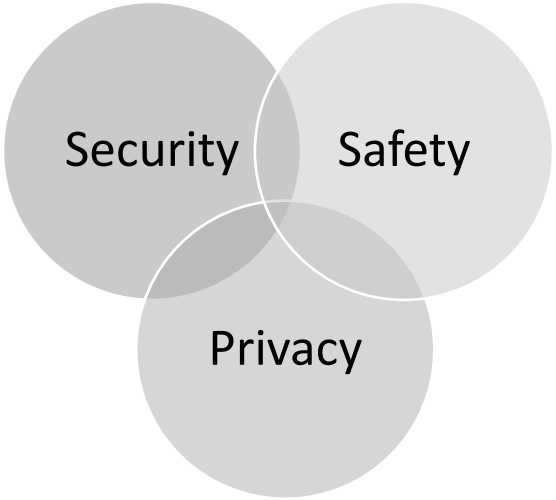
European Large-Scale Pilots Programme



Ecosystems



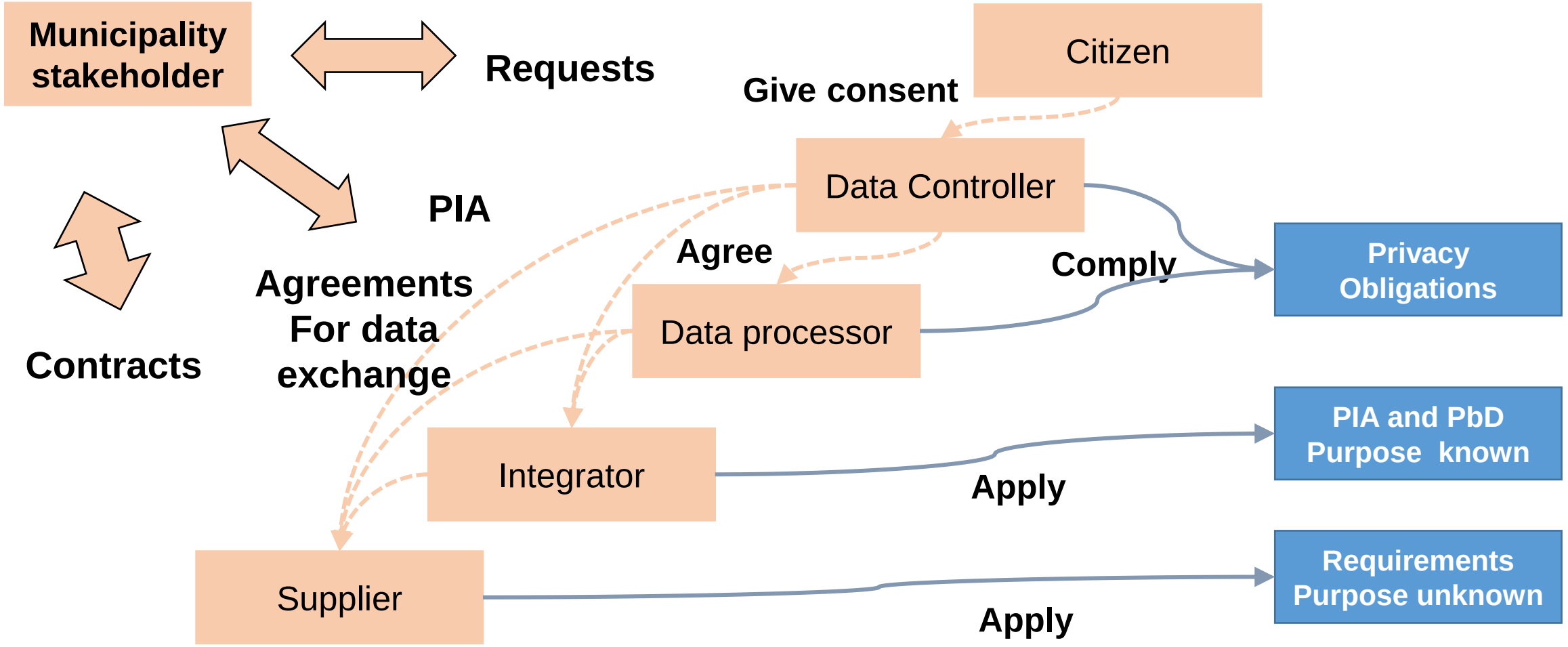
Domains



Concerns

Smart Cities Deal with Ecosystems

European Large-Scale Pilots Programme



Ecosystems Involve Supply Chains

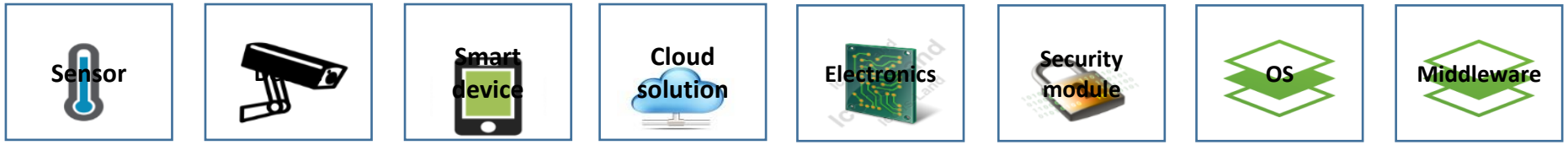
European Large-Scale Pilots Programme

Operator
Application 1

Operator
Application 2

Integrator

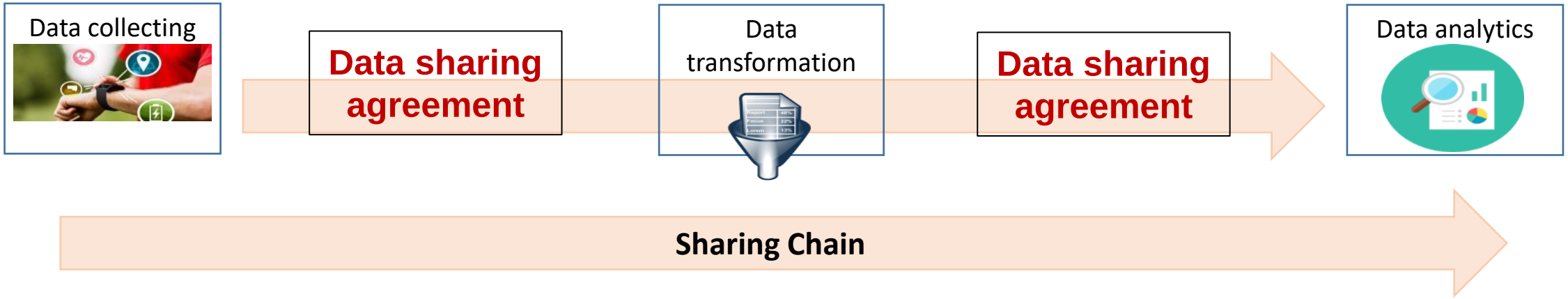
Supplier



Supply Chain

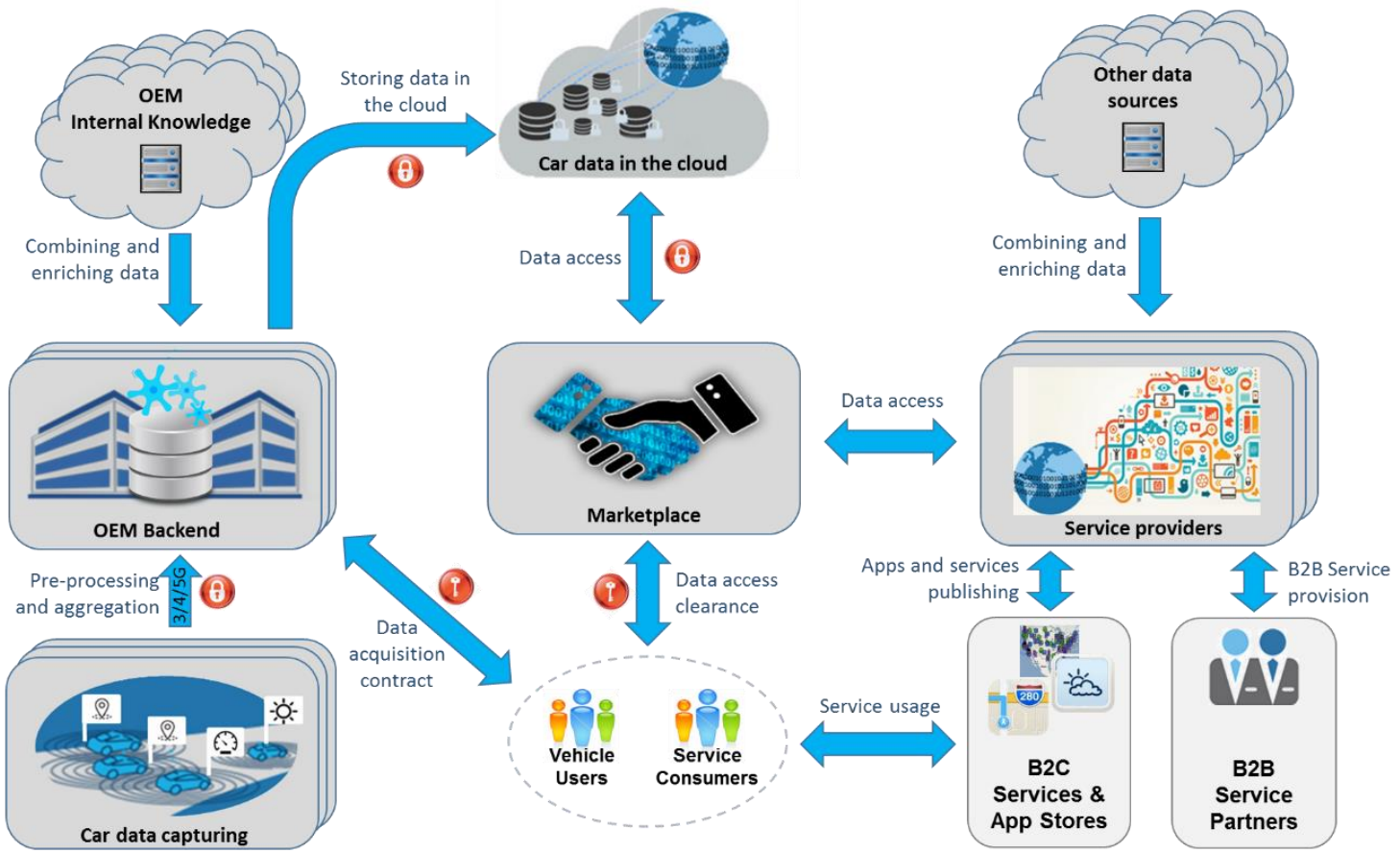
Ecosystems Involve Business Exchange

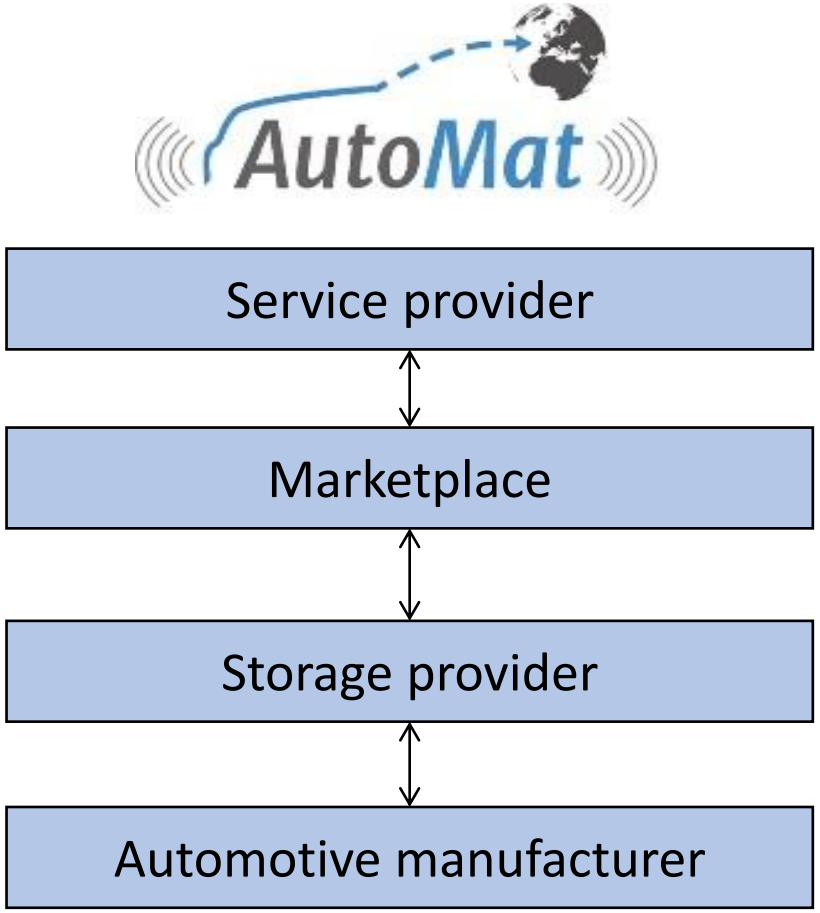
European Large-Scale Pilots Programme



Example of Big Data Ecosystem: AutoMat

European Large-Scale Pilots Programme

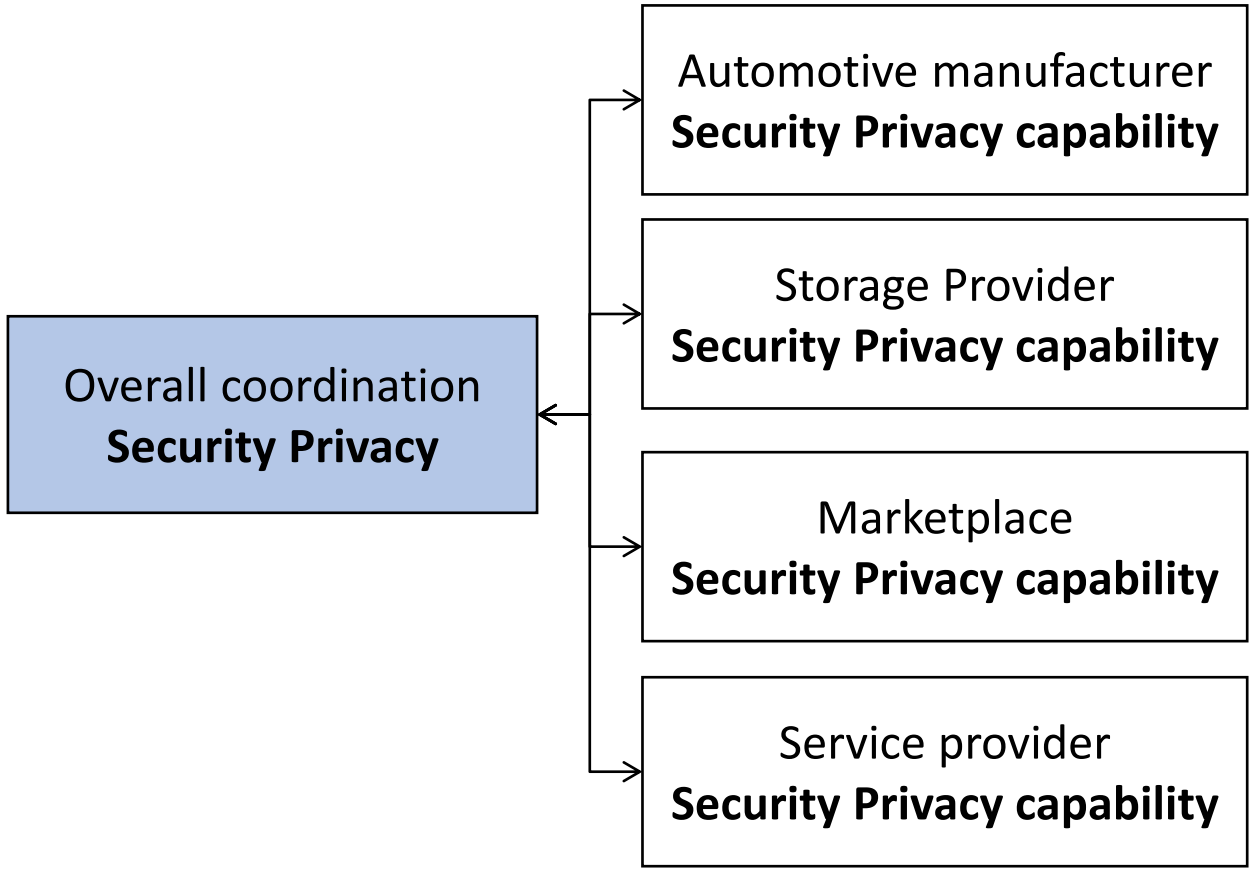




Need to coordinate between ecosystem stakeholders

European Large-Scale Pilots Programme

- Example of coordination needs
  - Privacy compliance
    - Global privacy impact assessment vs organisation PIA
    - PII tracking e.g. upon user consent removal
    - Data breach management
  - Cybersecurity compliance
    - Global risk analysis vs organisation risk analysis
    - Cybersecurity incident management



Impact on Standards Landscape

European Large-Scale Pilots Programme

Additional guidelines For ecosystems

Privacy Standards for Smart Cities
27570 Privacy guidelines

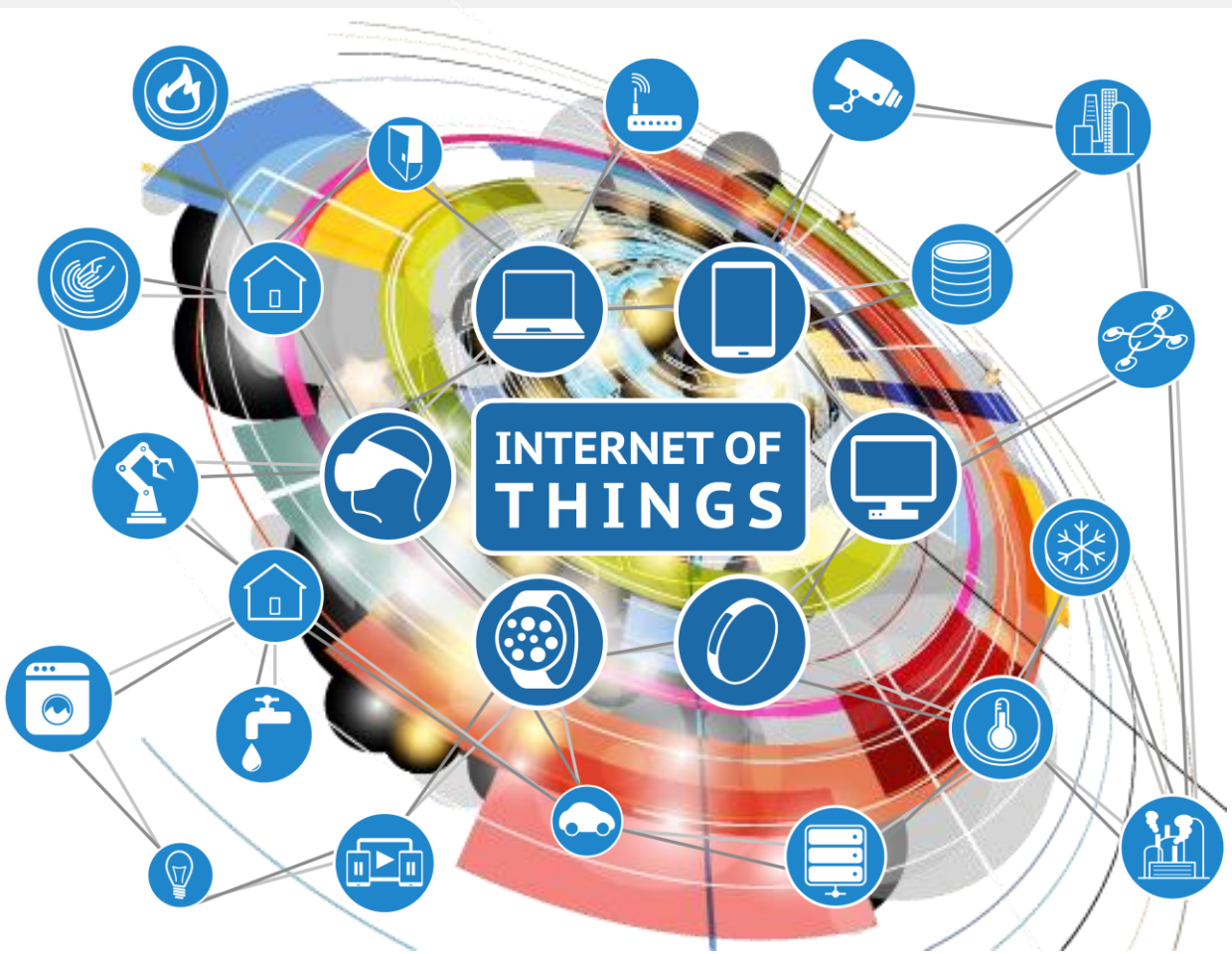
Privacy Standards for Big Data
20546-4 Security and privacy

Privacy Standards for IoT
27030 Security and privacy guidelines

General Privacy Standards
Privacy framework 29100
Privacy impact assessment 29134
Privacy engineering 27550
Code of practice 29151
Privacy Information management systems 27552
OASIS-PMRM

Thank You!

European Large-Scale Pilots Programme



www.european-iot-pilots.eu
www. create-iot.eu

@IOTEULSP
@CREATE-IoT
@IoT_euLSP
@CreateIoT_eu

The CREATE-IoT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732929.

email: antonio.kung@trialog.com

Introduction to smart city use case session

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

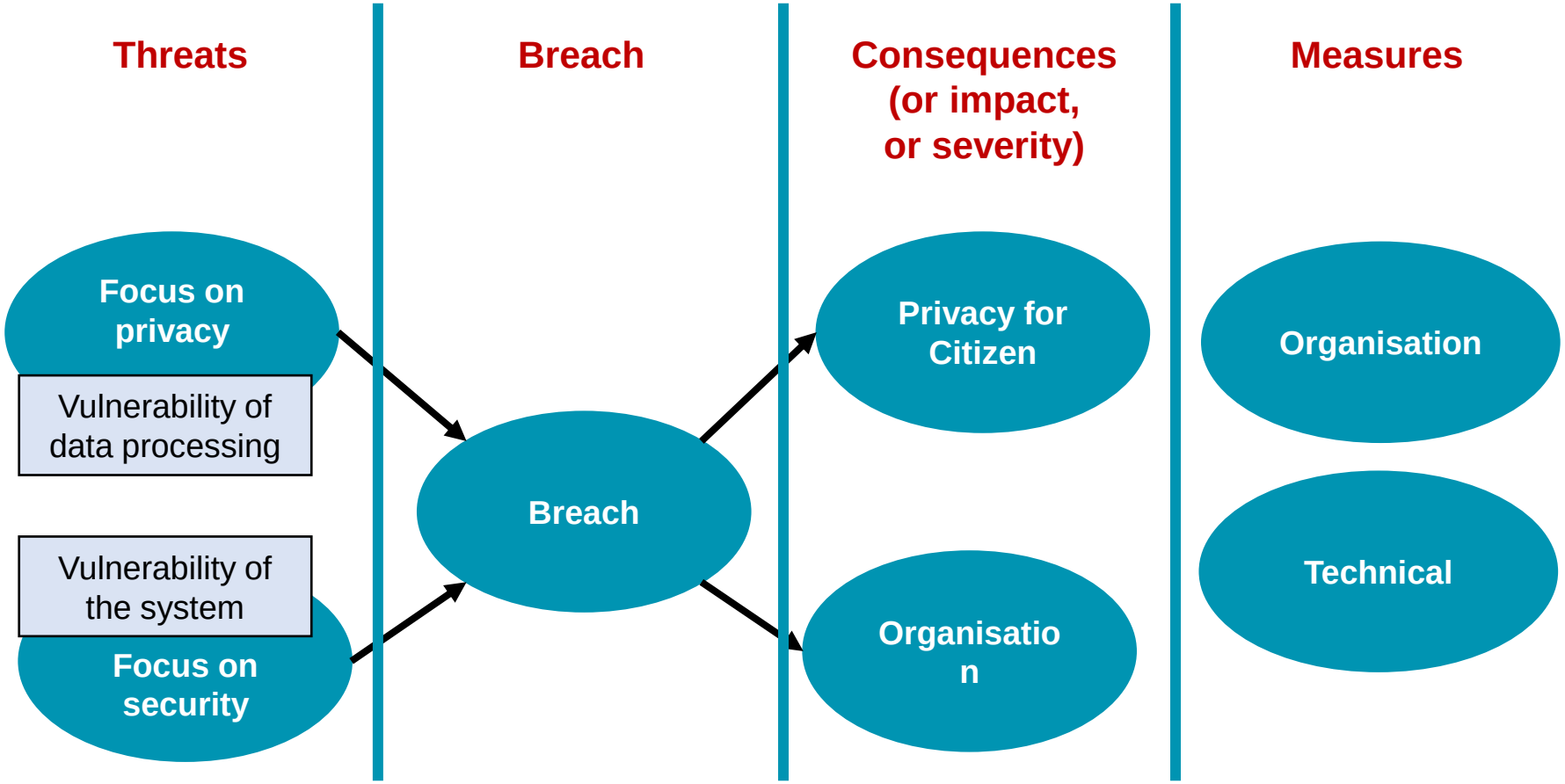
Context

European Large-Scale Pilots Programme

- Many such sessions carried out since 2017
- Participative approach
  - Citizen, Policy makers, Engineers
- Templates based on standards
- Content : impact analysis
  - Breaches
  - Threats and consequences
  - Measures

Security and privacy assessment (based on ISO/IEC 27550)

European Large-Scale Pilots Programme



Co-funded by the European Commission

Threats (based on LINDDUN and STRIDE)

European Large-Scale Pilots Programme

Property	Threat
Unlinkability	**L**inkability
Anonymity	**I**dentifiability
Plausible deniability	**N**on-repudiation
Undetectability and unobservability	**D**etectability
Confidentiality	**D**isclosure of information
Content awareness	**U**nawareness
Policy and consent compliance	**N**on compliance

Property	Threat
Authentication	**S**poofing
Integrity	**T**ampering
Nonrepudiation	**R**epudiation
Confidentiality	**I**nformation disclosure
Availability	**D**enial Of Service
Authorization	**E**levation of privilege

Risk map (based on CNIL guidelines)

European Large-Scale Pilots Programme

Maximum Impact	Must be avoided or reduced		A O Absolutely avoided or reduced	
Significant Impact				
Limited Impact	These risks may be taken		Must be reduced	
Negligible Impact				
	Negligible Likelihood	Limited Likelihood	Significant Likelihood	Maximum Likelihood

Example

- Breach: Alice attendance is made public
- Threat and consequence
  - Treat: Some one hacks into the attendance management system and retrieves the log of attendance
  - Consequence
    - Likelihood significant
    - Impact
      - for Alice could be maximum
      - For the organisation could be significant

A

O

Security Measures (based on ISO/IEC 27000)

European

Category	Sub-categories
Policies	Management direction
Organization	Internal organisation Mobile devices and teleworking
Human resource security	Prior to employment During employment Termination and change of employment
Asset management	Responsibility for assets Information classification
Access control	Business requirements of access control User access management User responsibilities System and application access control Media handling
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas Equipment

Category	Sub-categories
Operation security	Operational procedures and responsibilities Protection from malware Backup Logging and monitoring Control of operational software Technical vulnerability management Information systems audit considerations
Communication security	Network security management Information transfer
System acquisition, development and maintenance	Security requirements Security in development processes Test data
Suppliers relationships	Security in supplier relationships Supplier service delivery management
Incident management	Management of incidents and improvements
Business continuity	Information security continuity Redundancies
Compliance	Compliance (legal and contractual) Information security reviews

Privacy measures: data controllers (based on ISO/IEC 27552)

European Large-Scale Pilots Programme

Category	Control
Conditions for collection and processing	Identify and document purpose
	Identify lawful basis
	Determine when and how consent is to be obtained
	Obtain and record consent
	Privacy impact assessment
	Contracts with PII processors
	Records related to processing PII
Rights of PII principals	Determining PII principals rights and enabling exercise
	Determining information for PII principals
	Providing information for PII principals
	Provide mechanism to modify of withdraw consent
	Provide mechanism to object to processing
	Sharing the exercising of PII princ
	Correction or erasure
	Providing copy of PII processed
	Request management
	Automated decision taking

Privacy-by-design and by-default	Limit collection
	Limit processing
	Define and document PII minization and de-identification objectives
	Comply with data minimization and de-identification use
	PII de-identification and deletion
	Temporary failes
	Retention
	Disposal
	Collection procedures
	PII transmission controls
PII sharing, transfer and disclosure	Identify basis for PII transfer
	Countries and organisations to which PII might be transferred
	Records of transfer of PII
	Records of PII disclosure to third parties
	Joint controller

Privacy measures: data processors (based on ISO/IEC 27552)

European Large-Scale Pilots Programme

Category	Control
Conditions for collection and processing	Cooperation agreement
	Organization's purposes
	Marketing and advertising use
	Infringing instruction
	PII controller obligations
	Records related to processing PII
Rights of PII principals	Obligations to PII principals
Privacy-by-design and by-default	Temporary files
	Return transfer or disposal of PII
	PII transmission controls
PII sharing, transfer and disclosure	Basis for transfert of PII
	Countries and organisations to which PII might be transferred
	Records of PII disclosure to third parties
	Notification of PII disclosure requests
	Legally binding PII disclosures
	Disclosure of subcontractors used to process PII
	Engagement of a subcontractor to process PII
	Change of subcontractor to process PII

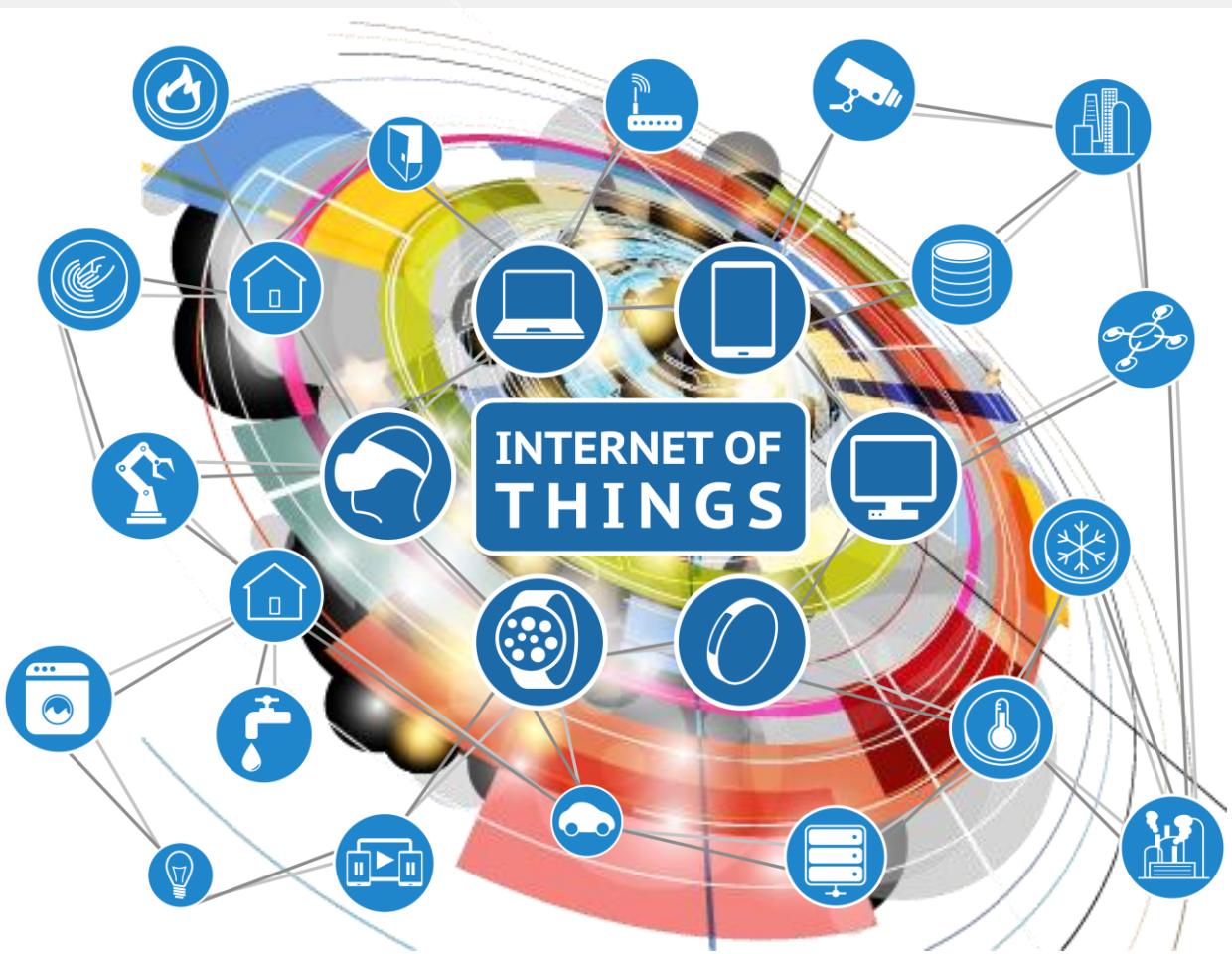
The five Results of a Workshop

European Large-Scale Pilots Programme

[1] Description of system component, data flow, data process	**[2] Breaches, Threats and consequences**
[3] Risk map	**[4] Measures**
[5] Conclusions / Actions	

Thank You!

European Large-Scale Pilots Programme



www.european-iot-pilots.eu
www. create-iot.eu

@IOTEULSP
@CREATE-IoT
@IoT_euLSP
@CreateIoT_eu

The CREATE-IoT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732929.

email: antonio.kung@trialog.com

Selection of Use Case

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Use case

European Large-Scale Pilots Programme

- Open data
- This part to be filled out with the audience

Legal and Ethical Compliance Viewpoint for Smart Cities

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Pasquale Annicchino, Archimede Solutions, Switzerland

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Smart city use case session: Breaches

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Use Case Breaches

European Large-Scale Pilots Programme

- Open data use case
  - Massive data leak
- This part to be filled out with the audience

Smart city use case session: Threats and Consequences

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Use Case Threat and Consequences

European Large-Scale Pilots Programme

- Open data use case
  - Weak anonymization
- This part to be filled out with the audience

Maximum Impact	Must be avoided or reduced		Absolutely avoided or reduced	
Significant Impact				
Limited Impact	These risks may be taken		Must be reduced	
Negligible Impact				
	Negligible Likelihood	Limited Likelihood	Significant Likelihood	Maximum Likelihood

Co-funded by the European Commission

Smart city use case session: Measures

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Use Case Measures

European Large-Scale Pilots Programme

- Open data use case
  - Set up an incident management scheme
- This part to be filled out with the audience

Security Measures for Use Case

Category	Sub-categories
Policies	Management direction
Organization	Internal organisation Mobile devices and teleworking
Human resource security	Prior to employment During employment Termination and change of employment
Asset management	Responsibility for assets Information classification
Access control	Business requirements of access control User access management User responsibilities System and application access control Media handling
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas Equipment

Category	Sub-categories
Operation security	Operational procedures and responsibilities Protection from malware Backup Logging and monitoring Control of operational software Technical vulnerability management Information systems audit considerations
Communication security	Network security management Information transfer
System acquisition, development and maintenance	Security requirements Security in development processes Test data
Suppliers relationships	Security in supplier relationships Supplier service delivery management
Incident management	Management of incidents and improvements
Business continuity	Information security continuity Redundancies
Compliance	Compliance (legal and contractual) Information security reviews

Privacy measures for Use Case: data controllers

European Large-Scale Pilots Programme

Category	Control
Conditions for collection and processing	Identify and document purpose
	Identify lawful basis
	Determine when and how consent is to be obtained
	Obtain and record consent
	Privacy impact assessment
	Contracts with PII processors
	Records related to processing PII
Rights of PII principals	Determining PII principals rights and enabling exercise
	Determining information for PII principals
	Providing information for PII principals
	Provide mechanism to modify of withdraw consent
	Provide mechanism to object to processing
	Sharing the exercising of PII princ
	Correction or erasure
	Providing copy of PII processed
	Request management
	Automated decision taking

Privacy-by-design and by-default	Limit collection
	Limit processing
	Define and document PII minization and de-identification objectives
	Comply with data minimization and de-identification use
	PII de-identification and deletion
	Temporary failes
	Retention
	Disposal
	Collection procedures
	PII transmission controls
PII sharing, transfer and disclosure	Identify basis for PII transfer
	Countries and organisations to which PII might be transferred
	Records of transfer of PII
	Records of PII disclosure to third parties
	Joint controller

Privacy measures for data processors

European Large-Scale Pilots Programme

Category	Control
Conditions for collection and processing	Cooperation agreement
	Organization's purposes
	Marketing and advertising use
	Infringing instruction
	PII controller obligations
	Records related to processing PII
Rights of PII principals	Obligations to PII principals
Privacy-by-design and by-default	Temporary files
	Return transfer or disposal of PII
	PII transmission controls
PII sharing, transfer and disclosure	Basis for transfert of PII
	Countries and organisations to which PII might be transferred
	Records of PII disclosure to third parties
	Notification of PII disclosure requests
	Legally binding PII disclosures
	Disclosure of subcontractors used to process PII
	Engagement of a subcontractor to process PII
	Change of subcontractor to process PII

Smart city use case session: Conclusions

IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

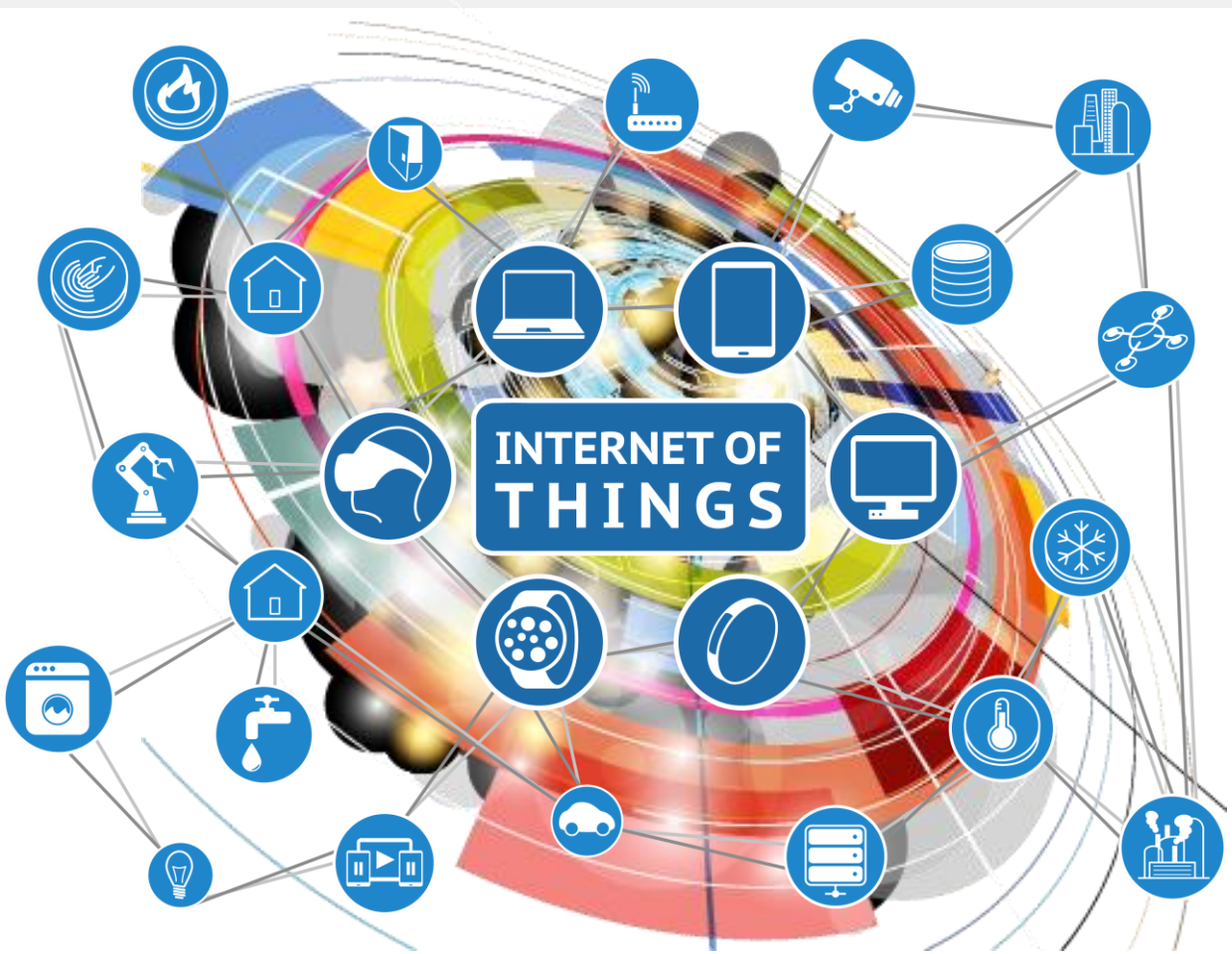
Conclusion

European Large-Scale Pilots Programme

- Open data use case
  - Set up an incident management scheme
- This part to be filled out with the audience

Thank You!

European Large-Scale Pilots Programme



www.european-iot-pilots.eu
www. create-iot.eu

@IOTEULSP
@CREATE-IoT
@IoT_euLSP
@CreateIoT_eu

The CREATE-IoT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732929.

email: antonio.kung@trialog.com